

Do Not Perform Arithmetic with Unvalidated Input

William L. Fithen, Software Engineering Institute [vita³]

Copyright © 2005 Carnegie Mellon University

2005-10-03

Careless modulo arithmetic can introduce vulnerability.

Description

According to [Seacord 05]:

Integers represent a growing and underestimated source of vulnerabilities in C and C++ programs. This is primarily because boundary conditions for integers, unlike other boundary conditions in software engineering, have been intentionally ignored. Most programmers emerging from colleges and universities understand that integers have fixed limits, but because these limits were either deemed sufficient, or because testing the results of each arithmetic operation was considered prohibitively expensive, violating integer boundary conditions has gone almost entirely unchecked in commercial software.

For an indepth coverage of this issue in C and C++, see [Safe Integer Operations](#)⁶.

References

- | | |
|---------------|--|
| [Blexim 02] | blexim. <i>Basic Integer Overflows</i> .
http://www.phrack.org/phrack/60/p60-0x0a.txt (2002). |
| [Hoglund 04] | Hoglund, Greg & McGraw, Gary. <i>Exploiting Software: How to Break Code</i> . Boston, MA: Addison-Wesley, 2004. |
| [Horovitz 02] | Horovitz, Oded. <i>Big Loop Integer Protection</i> .
http://www.phrack.org/phrack/60/p60-0x09.txt (2002). |
| [Howard 03a] | Howard, Michael. <i>Reviewing Code for Integer Manipulation Vulnerabilities</i> .
http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dncode/html/secure041020 (2003). |
| [Seacord 05] | Seacord, Robert C. <i>Secure Coding in C and C++</i> . Boston, MA: Addison-Wesley, 2005. |
| [Thompson 05] | Thompson, Herbert & Chase, Scott. <i>The Software Vulnerability Guide</i> . Charles River Media, 211-222. 2005. |

SEI Copyright

3. daisy:320 (Fithen, William L.)

6. daisy:312 (Safe Integer Operations)

Carnegie Mellon University SEI-authored documents are sponsored by the U.S. Department of Defense under Contract FA8721-05-C-0003. Carnegie Mellon University retains copyrights in all material produced under this contract. The U.S. Government retains a non-exclusive, royalty-free license to publish or reproduce these documents, or allow others to do so, for U.S. Government purposes only pursuant to the copyright license under the contract clause at 252.227-7013.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For inquiries regarding reproducing this document or preparing derivative works of this document for external and commercial use, including information about “Fair Use,” see the [Permissions](#)¹ page on the SEI web site. If you do not find the copyright information you need on this web site, please consult your legal counsel for advice.

Velden

Naam	Waarde
Copyright Holder	SEI

Velden

Naam	Waarde
is-content-area-overview	false
Content Areas	Knowledge/Guidelines
SDLC Relevance	Implementation
Workflow State	Publishable

1. <http://www.sei.cmu.edu/about/legal-permissions.html>